WHAT IS CLAIMED IS:

1. A system for securely transmitting Real Time Protocol voice packets during a communication session with a remote multimedia terminal adapter over an Internet protocol network, the system comprising:

a local multimedia terminal adapter receiving the voice packets, the local multimedia terminal adapter comprising,

a local key stream generator for generating a first key stream;

a packet encryptor that encrypts the voice packets using at least a portion of the first key stream to form encrypted voice packets;

the remote multimedia terminal adapter  receiving the encrypted voice packets, the remote multimedia terminal adapters further comprising,

a remote key stream generator for generating the first key stream in order to decrypt the encrypted voice packets; and

a packet decryptor decrypting the encrypted voice packets using the first key stream, wherein both  key stream generators are capable of generating a second key stream to prevent reuse of any portion of the first key stream during the communication session.

2. The system of claim 1 wherein the second key stream is generated when the system wishes to switch from a first to a second coder/decoder for compression/decompression of the voice packets.

3. The system of claim 1 wherein the second key stream is generated when a Message Authentication Code algorithm change occurs.

4. The system of claim 1 further comprising a local gateway controller for forwarding the encrypted packets through the Internet protocol network.

5. The system of claim 1 further comprising a remote gateway controller for receiving the encrypted packets from the Internet protocol network and for forwarding encrypted voice packets to the remote multimedia terminal adapter.

~~5.~~ 6. A system for communicating Real Time Protocol voice packets between a local and a remote location over an Internet protocol network, the system comprising:

a stream cipher module for encrypting the voice packets; and

a key stream generator for generating a first Real Time Protocol key stream, the stream cipher module employing the first key stream to encrypt the voice packets for forwarding to the remote location, the key stream generator producing a second Real Time Protocol key stream for encrypting the voice packets when the system wishes to switch from a first communication parameter to a second communication parameter, each of the first and second parameters being involved in the synchronization of the key stream.

~~6.~~ 7. The system of claim 6 wherein the first communication parameter is a first coder/decoder that compresses/decompresses the voice packets, and the second communication parameter is a second coder/decoder that compresses/decompresses the voice packets.

~~7.~~ 8. The system of claim 6 further comprising a synchronization source for synchronizing and enabling decryption of the voice packets at the remote location.

~~8.~~ 9. The system of claim 8 wherein the synchronization source is a time stamp on a voice packet.

~~9.~~ 10. The system of claim 9 further comprising a new time stamp sequence generated when the second Real Time Protocol key stream is generated.

~~10.~~ 11. The system of claim 6 wherein the second key stream is generated by re-executing the following key derivation function:

F(S, “End-End RTP Key Change <N>”)

where N is a counter incremented whenever a new set of Real Time Protocol keys is re-derived for the same media stream session;

F( ) is a one-way pseudo-random function used for the purpose of key derivation;

S is a shared secret - a random value shared between the two endpoints and is known only to those two endpoints and possibly a trusted server (e.g. gateway controller); and

"End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function F(), <N> stands for an ASCII representation of a decimal number, representing a counter.

~~11.~~ 12 The system of claim 6 wherein the second key stream is generated by re-executing the following key derivation function:

F(S, SSRC, "End-End RTP Key Change <N>") where:

S is a shared secret - a random value shared between the two endpoints and is known only to those two endpoints and possibly a trusted server (e.g. gateway controller);

SSRC is the synchronization source session identifier;

N is the counter of the number of key changes for the same SSRC value; and

"End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function F(), <N> stands for an ASCII representation of a decimal number, representing a counter.

~~12.~~ 13 A method for securely transmitting Real Time Protocol voice packets from a local to a remote location via a communication network, the method comprising:

generating a first Real Time Protocol key stream for encrypting the voice packets;

forwarding encrypted voice packets to the remote location;

generating a second Real Time Protocol key stream for encrypting the voice packets in response to a request to change communication parameters for the same media stream; and

forwarding voice packets encrypted with the second Real Time Protocol key stream to the remote location.

~~13.~~ 14 The method of claim 13 further comprising reinitializing a time stamp for synchronizing decryption of the voice packets.

~~14.~~ 15 The method of claim 13 wherein the step of generating a second Real Time Protocol key stream is by re-executing the following key derivation function:

F(S, “End-End RTP Key Change <N>”)

where N is a counter incremented whenever a new set of Real Time Protocol keys is re-derived for the same media stream session;

F( ) is a one-way pseudo-random function used for the purpose of key derivation;;

S is a shared secret - a random value shared between the two endpoints and is known only to those two endpoints and possibly a trusted server (e.g. gateway controller); and

"End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function F(), <N> stands for an ASCII representation of a decimal number, representing a counter.

~~15.~~ 16 The method of claim 13 wherein the step of generating a second Real Time Protocol key stream is by re-executing the following key derivation function:

F(S, SSRC, "End-End RTP Key Change <N>") where:

S is a shared secret - a random value shared between the two endpoints and is known only to those two endpoints and possibly a trusted server (e.g. gateway controller);

SSRC is the synchronization source session identifier;

N is the counter of the number of key changes; and

"End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function F(), <N> stands for an ASCII representation of a decimal number, representing a counter.

~~16.~~ 17 In a communication system having a gateway receiving communication sessions from two or more multimedia terminal adapters, a method for securely exchanging voice packets between the multimedia terminal adapters and the gateway, the method comprising:

generating a first Real Time Protocol key stream for encrypting the voice packets;

forwarding the voice packets encrypted with the first Real Time Protocol key stream to the gateway;

generating a second Real Time Protocol key stream for encrypting the voice packets in response to a collision detection wherein the multimedia terminal adapters have the same source identifier; and

forwarding voice packets encrypted with the second Real Time Protocol key stream to the remote location.

rule 1.126

~~17~~. 18 The method of claim 17 wherein the step of generating a second Real Time Protocol key stream is by re-executing the following key derivation function:

F(S, SSRC, "End-End RTP Key Change <N>") where:

S is a shared secret - a random value shared between the two endpoints and is known only to those two endpoints and possibly a trusted server (e.g. gateway controller);

SSRC is the synchronization source session identifier;

N is the counter of the number of key changes; and

"End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function F(), <N> stands for an ASCII representation of a decimal number, representing a counter.

~~18~~. 19 A system for securely transmitting voice packets during a communication session from a local location to a remote location over a communication network, the system comprising:

a means for generating a first key stream at the local location;

a means for encrypting the voice packets using at least a portion of the first key stream to form encrypted voice packets;

a means for forwarding the encrypted voice packets from the local location to the remote location;

a means for generating the first key stream at the remote location in order to decrypt the encrypted voice packets; and

a means for decrypting the encrypted voice packets using the first key stream, wherein both means for generating are capable of generating a second key stream to prevent reuse of any portion of the first key stream during the communication.

~~19~~. 20 The system of claim 19 wherein the second key stream is generated when the system wishes to switch from a first to a second coder/decoder for compression/decompression of the voice packets.

~~20~~. 21 The system of claim 19 wherein the second key stream is generated by re-executing the following key derivation function:

F(S, "End-End RTP Key Change <N>")

where N is a counter incremented whenever a new set of Real Time Protocol keys is re-derived for the same media stream session;

F( ) is a one-way pseudo-random function used for the purpose of key derivation;

S is a shared secret - a random value shared between the two endpoints and is known only to those two endpoints and possibly a trusted server (e.g. gateway controller); and

"End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function F(), <N> stands for an ASCII representation of a decimal number, representing a counter.

~~21.~~ 22 The system of claim 19 wherein the second key stream is generated by re-executing the following key derivation function:

F(S, SSRC, "End-End RTP Key Change <N>") where:

S is a shared secret - a random value shared between the two endpoints and is known only to those two endpoints and possibly a trusted server (e.g. gateway controller);

SSRC is the synchronization source session identifier;

N is the counter of the number of key changes; and

"End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function F(), <N> stands for an ASCII representation of a decimal number, representing a counter.

~~22.~~ 23 The system of claim 19 further comprising a means for synchronizing the voice packets.